UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,630	05/12/2008	Ernst Haselsteiner	AT03 0055 US1	1877

65913 7590 02/08/2010

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
02/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/574,630
Filing Date: May 12, 2008
Appellant(s): HASELSTEINER ET AL.

Mark A. Wilson
Registration No. 43,994
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed November 2, 2009 appealing from the Office action mailed June 4, 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

EP 1280042	PROUDLER	1-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-15 are rejected under 35 U.S.C. 102(a) as being anticipated by Proudler et al. (EP 1280042 A2).

Regarding claim 1, Proudler discloses:

A method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, comprising the following steps:

transmitting first authorization data of the hardware and/or software to a first unit (paragraph 0016-0019, 0029-0030, 0041, 0049-0051: *sends a nonce to the trusted device, and receives a response used to verify the trusted device*);

comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit (paragraph 0016: *identity and integrity metric are compared with expected values provided by a trusted party*)

authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit (paragraph 0016: *identity and integrity metric are compared with expected values provided by a trusted party, and if there is a match, the device is trusted*)

transmitting second authorization data of a data carrier to a second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*);

comparing the second authorization data in the second unit with second verification data stored in the second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*)

authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*)

wherein a direct data exchange is carried out between the first unit and the second unit (paragraph 0041, 0052: *communication between the trusted device and the platform after logical binding*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the direct data exchange between the first unit and the second unit comprises a transmission of encrypted data and a comparison and/or decryption of data transmitted between the first unit and the second unit (paragraph 0019, paragraph 0051: cryptographic processes).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the data exchange between the first unit and the second unit is carried out prior to an identification and/or verification of first authorization data of the hardware and/or software and of second authorization data of the data carrier (paragraph 0041, 0052: *communication between the trusted device and the platform after logical binding*).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein a central arithmetic unit of the first unit and a central arithmetic unit of the second unit jointly access at least one ROM memory one RAM memory and/or one non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein encryption of the first authorization data and of the second authorization data is carried out in the first unit and in the second unit (paragraph 0019, paragraph 0051: *cryptographic processes*).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the second authorization data are obtained from a smartcard or a tag or a label that forms the data carner (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Regarding claim 7, Proudler discloses:

A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, comprising:

a first unit for identifying and/or verifying the hardware and/or software of the appliance (paragraph 0016-0019, 0029-0030, 0041, 0049-0051: *sends a nonce to the trusted device, and receives a response used to verify the trusted device*), comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*), and

a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*),

wherein a communication interface is provided between the central arithmetic units of the first unit and the second unit (paragraph 0041: *communication between platforms*).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the memories of the first unit and of the second unit are formed by a ROM memory and a RAM memory and/or a non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 10 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the first unit and the second unit in each case comprise an encryption device (paragraph 0019, paragraph 0051: *cryptographic processes*).

Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the central arithmetic unit of the first unit and the central arithmetic unit of the second unit are combined to form a common central arithmetic unit which common central arithmetic unit has the integrated communication interface, and wherein the common central arithmetic unit is connected by an interface to the hardware and/or software that is to be identified and/or verified (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 12 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the interface to the external data carrier is designed for contactless communication with the external data carrier (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Claim 13 is rejected as applied above in rejecting claim 14. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the external data carrier is formed by a smartcard or a tag or a label (paragraphs 0032-0034: *label or a smart card*).

Claim 14 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

An appliance which comprises as hardware at least one central arithmetic unit which central arithmetic unit is designed to run software and to obtain data from an external data carrier cooperating with the appliance, wherein a circuit as claimed in claim 7 is coupled to the central arithmetic unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Proudler discloses:

An appliance as claimed in claim 14, wherein the central arithmetic unit of the appliance is coupled via an interface integrated in the central arithmetic unit of the appliance to the circuit integrated in the central arithmetic unit (paragraph 0030-0034).

(10) Response to Argument

The Appellant argues:

That Proudler does not disclose both first authorization data and verification data stored on a first unit and second authorization data and verification data stored on a second unit. The Examiner contends that Proudler does teach both a first and second unit and first and second authorization data. First, the Examiner contends that there is a first and a second unit disclosed in Proudler. The first unit is interpreted as being the measurement function of the trusted device (Figure 8, item 24, block 31: see paragraph 0029) which receives an integrity metric (authorization data from the computing platform (see paragraph 0029). The second unit is interpreted as being the authentication function block of the trust device (Figure 8, item 24, block 33) which authenticates the smart card via encryption/decryption and signature/verification (second authorization data) (see paragraphs 0029-0030). Second, the Examiner contends that there is first and second authorization data disclosed in Proudler. As disclosed above, the first authorization data is the integrity metric transmitted from the computing platform (hardware) to the first unit (see paragraph 0029). The second authorization data is interpreted as the authentication information transmitted between the smart card and the second unit (see paragraphs 0029-0030). Therefore, the Examiner contends that Proudler discloses a first and second unit, and a first and second authorization data.

The Appellant further argues:

That Proudler does not disclose multiple central arithmetic units jointly accessing a memory device. The Examiner contends that Proudler does disclose central arithmetic units jointly accessing a memory device. Proudler discloses that each of the blocks in the trusted device, including the authentication function block and the measurement function block, has access to appropriate volatile memory areas and/or non-volatile memory areas of the trusted device (see paragraph 0030). Both units have central arithmetic units because both the authentication block (which performs encryption/decryption and signature/verification) and the measure function block (which acquires and authenticates the integrity metric) perform arithmetic functions (paragraphs 0029-0030). Furthermore, the Examiner notes that there is no requirement that the central arithmetic units be separate or that there be multiple central arithmetic units, but just that each unit uses one. Therefore, the Examiner contends that Proudler does disclose central arithmetic units jointly accessing a memory device.

The Appellant further argues:

That Proudler does not disclose encrypting first and second authorization data. The Examiner contends that Proudler does disclose encrypting first and second authorization data. First, Proudler discloses that cryptographic processes are used to secure the data in the trust device where the first and second authorization devices are used (paragraph 0019). Second, Proudler also discloses receiving the integrity metric and the authentication information via a secure data transfer (see paragraph 0029), and a cryptographic function which encrypts and decrypts specified data (see paragraph 0030). Therefore, the Examiner contends that the secure data transfer and encrypting the data is analogous to encrypting first and second authorization data.

The Appellant further argues:

That Proudler does not disclose separate first and second units with separate central arithmetic units. The Examiner contends that Proudler does disclose a first and second unit with each comprising a central arithmetic unit. Both units have central arithmetic units because both the authentication block (which performs encryption/decryption and signature/verification) and the measure function block (which acquires and authenticates the integrity metric) perform arithmetic functions (paragraphs 0029-0030). Furthermore, the Examiner notes that there is no requirement that the central arithmetic units be separate or that there be multiple central arithmetic units, but just that each unit comprises one.

The Appellant finally argues:

That Proudler does not disclose that the first and second units are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory. The Examiner contends that Proudler does disclose such a common memory being formed between the first and second units. . Proudler discloses that each of the blocks in the trusted device, including the authentication function block and the measurement function block, has access to appropriate volatile memory areas and/or non-volatile memory areas of the trusted device (see paragraph 0030). Therefore, the Examiner contends that both the first and second units have access to this common volatile and non-volatile memory.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kaveh Abrishamkar

/Kaveh Abrishamkar/

Primary Examiner, AU 2431

01/28/2010

Conferees:

/Christopher A. Revak/

Primary Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431